

Appl. No. 10/058,214

Reply to Office Action of: March 24, 2005

Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (currently amended) A method of providing a point multiple in an elliptic curve cryptosystem for performing cryptographic operations, said point multiple being derived from a scalar and a point on an elliptic curve having an equation of the form $y^2 + xy = x^3 + a_1x^2 + 1$, where a_1 is either 0 or 1, said method comprising the steps of:
 - a) obtaining a pair of coefficients derived from a truncator of said elliptic curve;
 - b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve;
 - c) computing said point multiple using said representation of said scalar and a Frobenius mapping τ ; and
 - d) providing said point multiple to said elliptic curve cryptosystem for use in said cryptographic operations.
2. (original) A method according to claim 1, wherein said pair of coefficients corresponds to an approximation of the inverse of said truncator.
3. (original) A method according to claim 2, wherein said approximation is determined by a significance parameter.
4. (original) A method according to claim 1, wherein said representation of said scalar is equivalent to said scalar modulo said truncator.
5. (original) A method according to claim 2, further comprising the step of computing a quotient derived from said pair of coefficients and said scalar and using said quotient to perform the step of computing said representation of said scalar.

BEST AVAILABLE COPY

Appl. No. 10/058,214

Reply to Office Action of: March 24, 2005

6. (original) A method according to claim 5, wherein said quotient is equivalent to a product of said scalar and said approximation of said inverse of said truncator.
7. (original) A method according to claim 6, wherein said representation of said scalar is equivalent to a remainder after division of said scalar by said truncator.
8. (currently amended) A method according to claim 1, wherein said truncator is $\frac{\tau^m - 1}{\tau - 1}$,
wherein m is the extension degree of a finite field over which said elliptic curve is defined.
9. (currently amended) A method of computing a key for use in a cryptographic system, said key being derived from a scalar and a point on an elliptic curve having an equation of the form $y^2 + xy = x^3 + a_1x^2 + 1$, where a_1 , is either 0 or 1, said method comprising the steps of:
 - a) obtaining a pair of coefficients derived from a truncator of said elliptic curve;
 - b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve;
 - c) computing [[said]] a point multiple using said representation of said scalar and a Frobenius mapping $\tau[[.]]$; and
 - d) using said point multiple for computing said key for use in said cryptographic system.
10. (currently amended) In a method of computing an elliptic curve digital signature requiring a point multiple for use in a cryptographic system, the improvement comprising computing said point multiple by the steps of:
 - a) obtaining a pair of coefficients derived from a truncator of said elliptic curve;
 - b) computing a representation of said scalar from said pair of coefficients, said scalar, and said truncator of said elliptic curve;
 - c) computing said point multiple using said representation of said scalar and [[said]] an endomorphism of said elliptic curve $[[.]]$; and

BEST AVAILABLE COPY

Appl. No. 10/058,214

Reply to Office Action of: March 24, 2005

d) using said point multiple for computing said elliptic curve digital signature for use in said cryptographic system.

11. (original) A data carrier containing computer executable instructions for performing a method according to claim 1.
12. (original) A cryptographic system performing a method according to claim 1.

BEST AVAILABLE COPY